National Aeronautics and Space Administration

Johnson Space Center's Risk and Reliability Analysis Group

2008 Annual Report

TABLE OF CONTENTS

FOREWORD

The Johnson Space Center (JSC) Safety & Mission Assurance (S&MA) Directorate's Risk and Reliability Analysis Group provides both mathematical and engineering analysis expertise in the areas of Probabilistic Risk Assessment (PRA), Reliability and Maintainability (R&M) analysis, and data collection and analysis. The fundamental goal of this group is to provide National Aeronautics and Space Administration (NASA) decision-makers with the necessary information to make informed decisions when evaluating personnel, flight hardware, and public safety concerns associated with current operating systems as well as with any future systems.

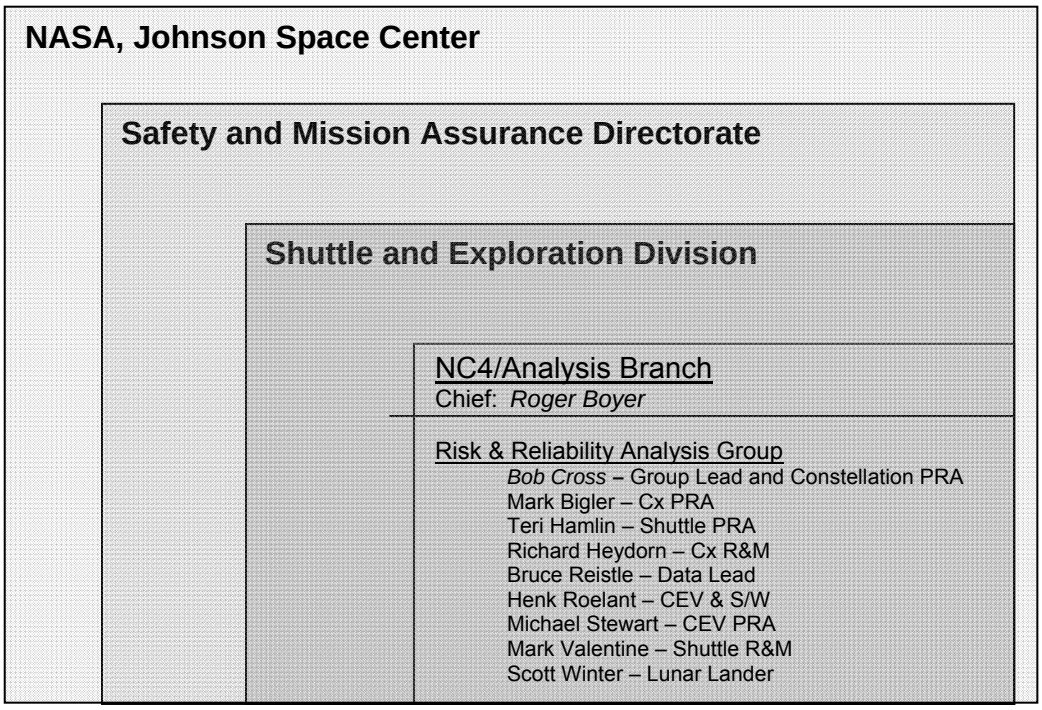
The Analysis Group includes a staff of statistical and reliability experts with valuable backgrounds in the statistical, reliability, and engineering fields. This group includes JSC S&MA Analysis Branch personnel as well as S&MA support services contractors, such as Science Applications International Corporation (SAIC) and SoHaR. The Analysis Group's experience base includes nuclear power (both commercial and navy), manufacturing, Department of Defense, chemical, and shipping industries, as well as significant aerospace experience—specifically in the Shuttle, International Space Station (ISS), and Constellation Programs. The Analysis Group partners with project and program offices, other NASA centers, NASA contractors, and universities to provide additional resources or information to the group when performing various analysis tasks. The JSC S&MA Analysis Group is recognized as a leader in risk and reliability analysis within the NASA community. Therefore, the Analysis Group is in high demand to help the Space Shuttle Program (SSP) continue to fly safely, assist in designing the next generation spacecraft for the Constellation Program (CxP), and promote advanced analytical techniques.

The Analysis Section's tasks include teaching classes and instituting personnel qualification processes to enhance the professional abilities of our analysts as well as performing major probabilistic assessments used to support flight rationale and help establish program requirements. During 2008, the Analysis Group performed more than 70 assessments. Although all these assessments were important, some were instrumental in the decision-making processes for the Shuttle and Constellation Programs. Two of the more significant tasks were the Space Transportation System (STS)-122 Low Level Cutoff PRA for the SSP and the Orion Pad Abort One (PA-1) PRA for the CxP. These two activities, along with the numerous other tasks the Analysis Group performed in 2008, are summarized in this report. This report also highlights several ongoing and upcoming efforts to provide crucial statistical and probabilistic assessments, such as the Extravehicular Activity (EVA) PRA for the Hubble Space Telescope service mission and the first fully integrated PRAs for the CxP's Lunar Sortie and ISS missions.

Roger L. Boyer
JSC S&MA Analysis Branch Chief
2101 NASA Parkway, Mail Code NC
Houston, Texas 77058
roger.l.boyer@nasa.gov
281.483.6070

INTRODUCTION

The Risk and Reliability Analysis Group was formed in 2003, under a general reorganization that formed the S&MA Directorate from the former Safety, Reliability, and Quality Assurance (SR&QA) Directorate at JSC. The Analysis Group is part of the Analysis Branch in the Shuttle and Exploration Division. The figure below shows the Analysis Group's organizational structure within JSC.



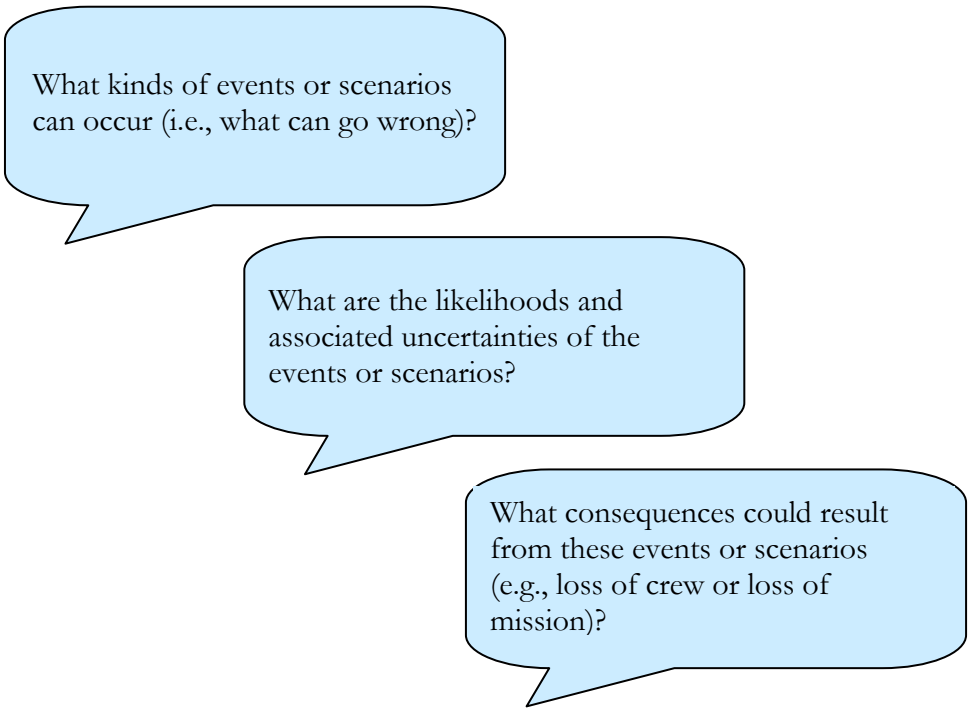
The NASA Procedural Requirements, *NASA Space Flight Program and Project Management Requirements* (NPR 7120.5D), March 06, 2007, establishes the requirement for risk management and analysis, more specifically PRA, to be used in all NASA projects and programs. The NASA Policy Directive, *NASA Reliability and Maintainability (R&M) Program Policy* (NPD 8720.1B), April 29, 2004, establishes a similar requirement for R&M analyses. The Analysis Group assists NASA programs and projects in meeting these obligations to ensure decisions concerning risks are informed, vehicles are safe and reliable, and program/project requirements are realistic and realized.

Probabilistic risk assessment, reliability and maintainability analysis, and data collection enable the Analysis Group to provide crucial reliability and failure information that NASA uses to support many of its safety-related decisions.

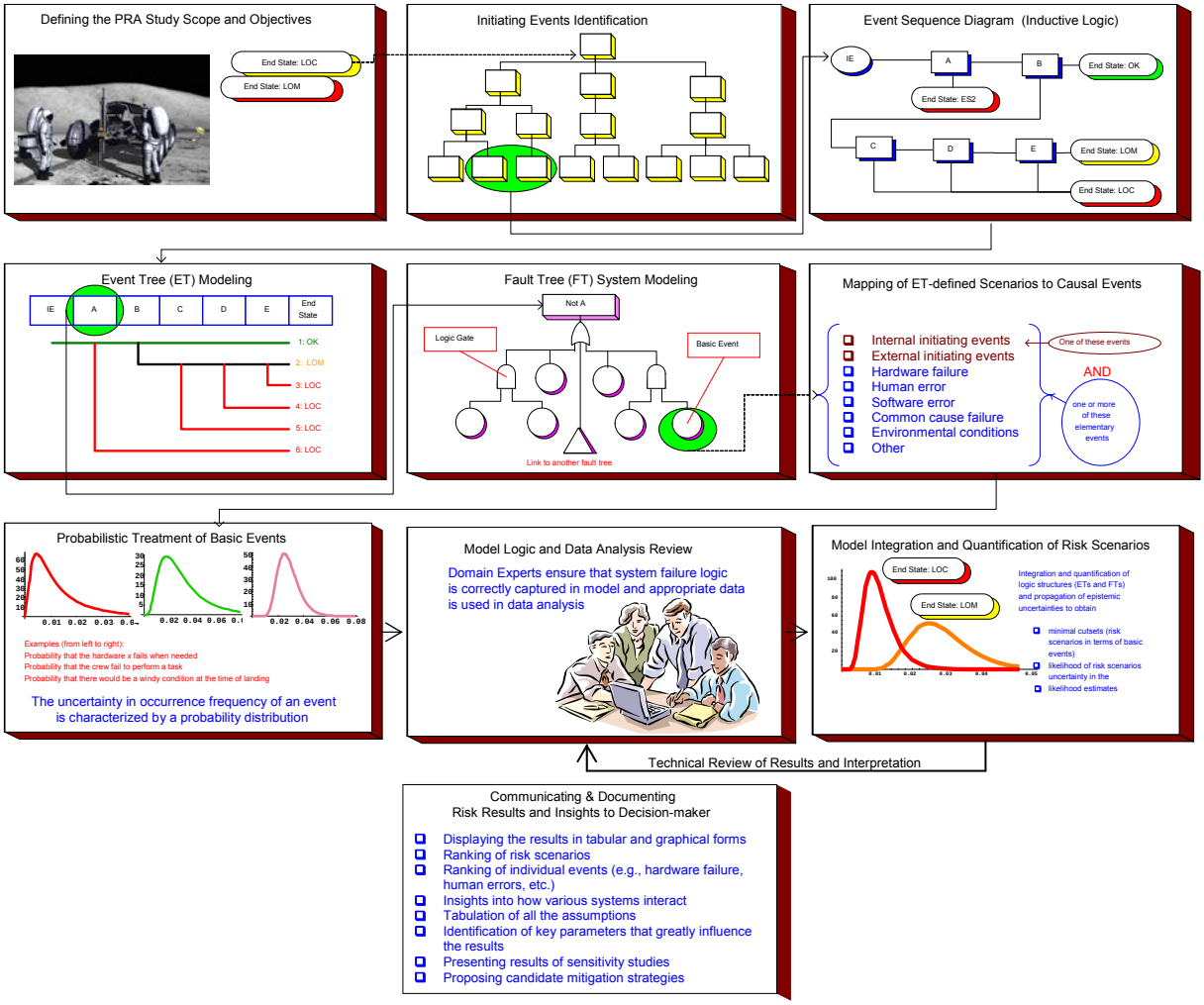
PRA

PRA is a comprehensive, structured, and disciplined approach for identifying, analyzing, and quantifying risks in engineered systems. PRA is primarily used as a decision support tool that uncovers design and operational weakness in engineered systems and then helps to systematically identify and prioritize safety improvements. PRAs must adequately represent the system design and operation as well as use standard and consistent PRA methods, practices, and applications. The complexity of a PRA is dependent on the complexity of the system being assessed and the questions to be answered. Complex system assessments require a team of PRA analysts and domain experts working together. The purpose and scope of a PRA drives the selection of PRA methods used for the analysis. The SSP uses PRA to assess mission risks as an input to its risk-informed decision-making process. The CxP and its project offices are using PRA during the conceptual phase and will continue using PRA throughout the life of the program to evaluate mission, system, element, and subsystem level risks both within and across projects. PRA is also used to perform focused risk studies. The knowledge gained about the risks to a system may then be used by management to cost-effectively improve the system's safety and performance in the face of uncertainties by making risk-informed decisions. If a PRA is performed early in the design and development cycle and the engineering and operations communities are actively engaged in performing the PRA, the PRA becomes an effective design tool for verifying risk requirements, performing risk trade studies, and reducing uncertainties.

In general, PRA is a process that seeks answers to three basic questions:



The figure below provides an overview of the PRA process.



The following paragraphs summarize PRA services the Analysis Group provides as well as some of the PRA tools they use.

Scenario Modeling uses inductive logic and probabilistic tools such as Event Sequence Diagrams (ESDs) and event trees to model each scenario. ESDs help the analysts and the review team identify the failure logic associated with the system or scenarios being developed. Event trees are developed from the ESDs to quantify the failure scenarios.

Failure Modeling uses deductive logic and probabilistic tools called fault trees to model each failure (or its complement, success) for a pivotal event in a failure scenario. Fault trees consist of three parts. The topmost element (top event) is a given pivotal event defined in a failure scenario. The second part of the fault tree consists of intermediate events that cause the top event. These events are linked through logic gates (i.e., AND gates and OR gates) to the basic events. The basic events are the third part of the fault tree, and their occurrence ultimately causes the top event.

Quantification and Integration is a process that uses an integrated PRA computer program to logically link and quantify the fault trees appearing in the path of each scenario. The frequency of occurrence for each end state in the event tree is the product of the initiating event's frequency and the (conditional) probabilities of the pivotal events along the scenario path linking the initiating event to the end state. The scenarios are then grouped according to the end state of the scenario defining the consequence. Finally, all end states are then grouped (i.e., their frequencies are summed into the frequency of a representative end state).

Uncertainty Analysis is part of the quantification process that evaluates the degree of knowledge or confidence in the calculated numerical risk results. Monte Carlo simulation methods are generally used to perform uncertainty analysis; although, other methods exist.

Sensitivity Analysis is frequently performed in a PRA to indicate analysis inputs or elements whose value changes cause the greatest changes in partial or final risk results. Sensitivity analysis identifies system components that, if modified, will have a greater impact on the overall system risk.

Importance Ranking is a special technique used in some PRA applications to identify the lead, or dominant, contributors to risk in accident sequences or scenarios by listing the lead contributors in decreasing order of importance. This process is generally performed first at the fault tree level and then at the event tree levels. Analysts usually use an integrated PRA computer program to establish the different types of risk importance measures in the importance ranking process.

R&M Analysis

Reliability engineering assesses the probability that a given component or system will operate as designed. Maintainability engineering assesses and verifies the system design characteristics to reduce the need for maintenance and ensure downtime is minimized when maintenance action is necessary. R&M analysis results are used to allocate design resources, focus operations on potential trouble areas, and identify requirements for spares inventories.

Reliability engineering also includes a process called trending, which assesses the reliability performance of systems and components during their missions and identifies changes in reliability performance over time. Through design evaluation, (probabilistic) modeling, analysis, and testing; reliability engineers work to improve the dependability of NASA systems. Reliability analyses are used to support PRA and logistics.

The following paragraphs summarize R&M services the Analysis Group provides as well as some of the R&M tools they use.

Physics of Failure Analysis identifies the underlying physical processes and mechanisms that cause failure. This analysis helps minimize the risk of failures by enabling analysts and decision-makers to understand the relationship between failures and their driving parameters (environmental, manufacturing process, material defects, etc.). Physics of failure analysis is useful throughout all phases of a program from technology development and design to operations.

Root Cause Analysis ensures that problems are systematically evaluated and corrected. The key element in a root cause analysis is a good Problem Reporting and Corrective Action (PRACA) System. PRACA is a closed-loop system for documenting hardware and software anomalies, analyzing their impact on R&M, and tracking them to their resolution. PRACA is a prime data source for program- and project-specific failure histories.

Reliability Assurance Plans identify the activities essential in assuring reliability performance requirements are met during design, production, and product assurance activities. These plans are written during program/project planning and apply throughout the program's/project's life. Adherence to these plans ensures that design risks are balanced against the program's/project's constraints and objectives.

Reliability Modeling uses prediction, allocation, and modeling tasks to identify inherent reliability characteristics. Reliability modeling aids in evaluating the reliability of competing designs. It is used in design and in operations when failure rates are needed for tradeoff studies, sparing analysis, etc. Reliability modeling results are often used to establish procurement specifications.

Trend Analysis examines past results and evaluates variation in data with the ultimate objective of forecasting future events. Typically, trend analysis is used in the operational phase of a program to provide a means for assessing whether a system or component is in its break-in, operational, or wear-out phase. Trend analysis is also useful in determining if an external factor is affecting a system or component.

Regression Analysis evaluates the relationship between a dependent variable and one or more independent variables and generates an equation to describe the effect of one variable upon another. The most commonly used method for modeling the relationship is least squares, but other methods are available. The least squares method assesses the "statistical significance," or the degree of confidence, that the true relationship is close to the estimated relationship. Once the relationship, or model, between the variables is obtained, the model can be used to further investigate the root cause or to predict the value of the dependent variable.

Reliability Growth is the improvement in a reliability parameter over a period of time due to changes in product design or the manufacturing process. It occurs by surfacing failure modes and implementing effective corrective actions. Reliability growth management involves systematically planning for reliability achievement as a function of time and other resources, and controlling the ongoing rate of achievement by reallocating these resources based on comparisons between planned and assessed reliability values.

Weibull Analysis matches historical failure and repair data to appropriate Weibull distributions. These distributions represent the failure or repair characteristics of a given failure mode and may be assigned to failure models that are attached to blocks in a reliability block diagram or events in a fault tree diagram. Weibull analysis results are typically given by two parameters that describe the distribution curve. These parameters are β, the shape parameter, and η, the scale parameter (characteristic life). β is useful in determining the failure characteristics of the data. If the failure rate is increasing, then β is greater than 1; if the failure rate is decreasing, then β is less than 1; or if the failure rate is constant, then β equals 1.

Simulation is a problem solving technique that approximates the probability of certain outcomes by running multiple trial runs, called simulations, using random variables. Simulation is often used when the system to be modeled is too complex to develop a closed-formed mathematical solution for the reliability problem. The three classic types of reliability simulators are: Monte Carlo, reliability block diagram, and queuing.

Data Collection, Analysis, and Management

Data is the essential component (the life blood) of PRA and R&M analysis. Various types of data must be collected and processed for use throughout the PRA process and in R&M analyses. NASA gathers data from a variety of sources within and outside of NASA. One of the primary data sources for each NASA program is its PRACA System. The PRACA Database records typically provide the failure data for the program. External data sources may include the Reliability Analysis Center Automated Databook's Nonelectronic Parts Reliability Data and Electronic Parts Reliability Data, the National Transportation Safety Board, the Nuclear Computerized Library for Assessing Reactor Reliability, and other sources. The Analysis Group analyzes both internal and external data for the problem, system, or component under study to support PRAs and R&M analyses. Once data is collected for a particular study, the Analysis Group stores or maintains the data so it can be retrieved and referenced for future purposes.

Data collection and analysis proceeds in parallel, or in conjunction, with PRA and R&M analysis. Data is assembled to quantify accident scenarios and contributors. Data includes, but is not limited to, component failure rates, repair times, initiating event probabilities, structural failure probabilities, human error probabilities, process failure probabilities, and common cause failure probabilities. Uncertainty bounds and uncertainty distributions are also collected and developed in the data collection process.

2008 ANALYSIS TASKS

The Analysis Group supports projects and programs from the conceptual stage, through operations, and decommissioning. JSC S&MA currently supports three major programs: SSP, ISS, and CxP. The Analysis Group plays a primary role in supporting the Shuttle and Constellation Programs along with their Orbiter, Orion, Lunar Lander, and EVA Projects. The Analysis Group also supports the Mission Operations, Engineering, Life Sciences, and Flight Crew Directorates at JSC. This report briefly summarizes the activities within each program the Analysis Group supports.

Shuttle

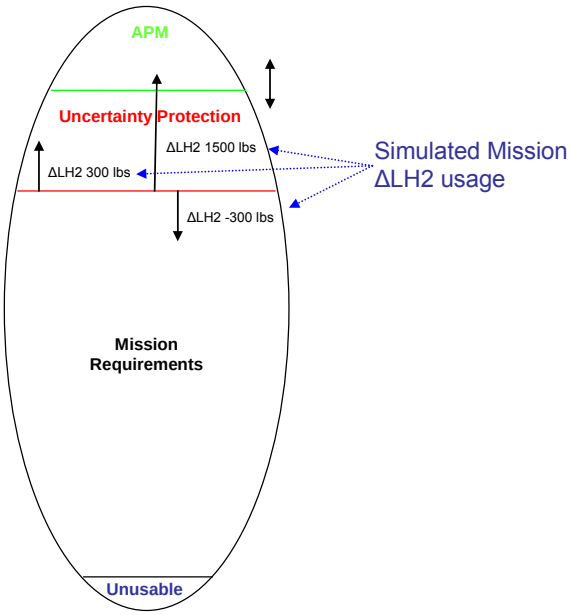
First launched in April 1981, the Shuttle is the only spacecraft capable of delivering and returning large payloads and scientific experiments to and from space. It is scheduled for decommissioning in 2010 upon completion of the ISS construction. Today, the Shuttle fleet is comprised of the Discovery, Atlantis, and Endeavour Orbiters. Shuttle flights have supported both Space Station Mir and the ISS; deployed and serviced the Hubble Space Telescope; and deployed planetary spacecraft to study Jupiter, Venus, and the sun. In the Orbiters' onboard laboratories, hundreds of experiments have helped scientists study the effects of reduced gravity on materials, plants, animals, and human beings to benefit life on Earth.

When describing the Analysis Group's involvement with Shuttle support, it is important to first explain the Shuttle PRA because many of the risk trades and special assessments performed for the SSP use the Shuttle PRA results as a foundation. The Shuttle PRA is the only PRA recognized by the SSP and NASA. It is a "living" PRA that is periodically updated due to increased operation and failure history changes, operational procedures and process changes, or system design changes. The Shuttle PRA was initially developed by a team of analysts and domain experts from across the SSP that were led by the Analysis Group. Originally baselined in 2003, after peer review by an external team, the Shuttle PRA is now in its sixth update. The Shuttle PRA includes over 10,000 pages of documentation, which is also maintained by the Analysis Group. The Shuttle PRA represents a substantial amount of work and Shuttle knowledge integrated into a single assessment that has supported many SSP risk-informed decisions over the years and will support the remainder of the program.

The following summaries highlight the PRA, R&M, and data management tasks the Analysis Group performed for the SSP in 2008.

Shuttle PRA Tasks

Low Level Cutoff PRA

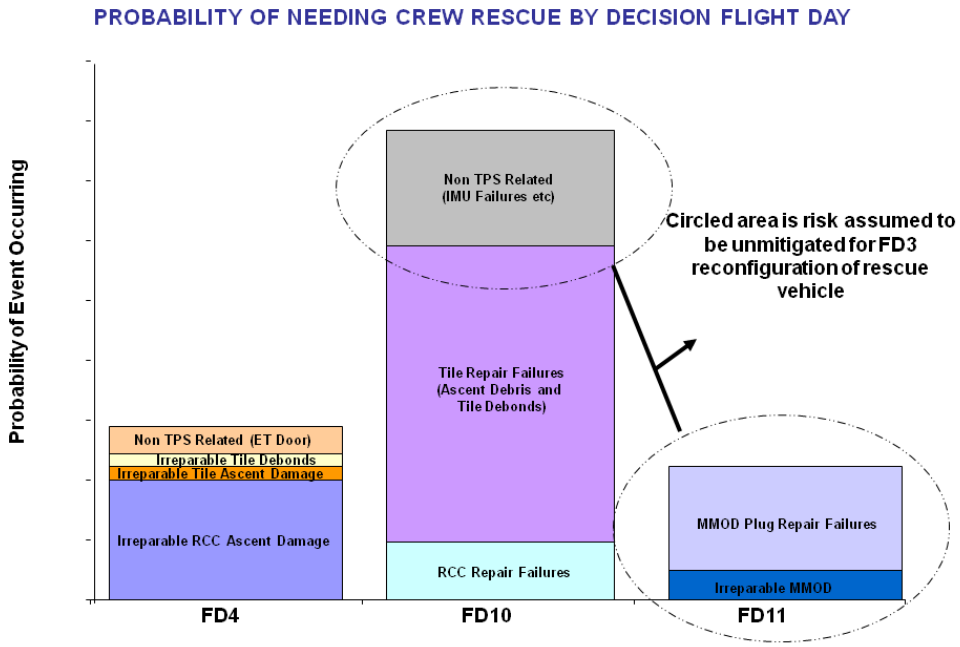


The Engine Cutoff (ECO) sensors provide Low Level Cutoff (LLCO) protection for the Space Shuttle Main Engines (SSMEs). The fuel (liquid hydrogen) ECO sensors are located in the External Tank, and the oxidizer (liquid oxygen) ECO sensors are located in the Orbiter. If either the fuel or oxidizer fluid levels drop below a certain point, the SSME turbo pumps may cavitate—resulting in a catastrophic event. The liquid hydrogen ECO sensors have plagued the SSP in recent years. Following the Columbia accident and in preparation for STS-114, several liquid hydrogen ECO sensor failures were observed. Due to the ECO sensors' wide-sweeping effects, significant analyses were performed across the program. The Analysis Group performed a PRA for the ECO sensor scenarios based on the data available at that time and showed that common cause failures occurred when unexplained anomalies were added to the known failures. The Analysis Group's assessment focused on ECO sensor failures, and the probability of a LLCO was based upon a simple Chi-Square model using zero failures. Although the assessment estimates were believed to be conservative at the time, a better estimate was not available.

In December 2007, STS-122 experienced a complete loss of the liquid hydrogen ECO sensor system. The Shuttle Program Manager asked the Analysis Group to provide a definitive estimate for the LLCO probability. The LLCO model needed to provide enough detail to clearly show the impact of potential improvements such as increased Ascent Performance Margin (APM), and the model needed to be accepted by the SSP community. The Analysis Group lead a team that consisted of personnel from Johnson Space Center (JSC)/Kennedy Space Center (KSC)/Marshall Space Flight Center (MSFC) S&MA, SSME, Systems Engineering and Integration (SE&I), Pratt and Whitney Rocketdyne (PWR), NASA Engineering and Safety Center (NESC), and Boeing to create a Monte Carlo model that simulated delta liquid hydrogen consumption. A delta liquid hydrogen consumption greater than the available Flight Performance Reserve (FPR), Fuel Bias (FB), and APM will result in an LLCO. The LLCO model results were presented to the Program Requirements Control Board (PRCB), and the SSP used the results to make informed decisions regarding the liquid hydrogen ECO sensor system.

Hubble Space Telescope (HST) Rescue Vehicle Release

In October of 2008, NASA planned to service the HST. When adding the HST service mission to the manifest in 2006, NASA decided to provide a rescue capability with a Shuttle waiting on the second launch pad since the ISS would not be available for Contingency Shuttle Crew Support (CSCS). The planned HST rescue vehicle was the STS-126 vehicle, which was planned to launch November 10, 2008. Due to the potential for launch delays, which could slip the STS-126 launch to within a beta window cutout beginning on November 29th and ending on December 17th; the Shuttle Program Manager considered releasing the HST rescue vehicle early to begin processing the vehicle for the STS-126 mission. A beta window cutout is a period of time when the Shuttle cannot dock with the ISS due to thermal constraints. Releasing the rescue vehicle early would make crew rescue unavailable if it were needed late in the mission (e.g., following late mission inspection). The Analysis Group used a previously developed simulation model to assess manifest options as a basis for performing a schedule risk assessment to compare against the increased risk for Loss of Crew (LOC) due to losing the HST crew rescue capability for late mission "call-ups." The simulation model considered ground operations and the various risk contributors to launch availability, such as weather- and hardware failure-related delays. The analysis results revealed the magnitude of the schedule risk improvement gained by releasing the rescue vehicle compared to the increase in HST LOC. The HST rescue vehicle release analysis was instrumental in assisting the Shuttle Program Manager with making an informed decision not to release the HST rescue vehicle. Ultimately, an HST failure delayed the HST mission to May 2009, and STS-126 was launched before the beta window cutout.

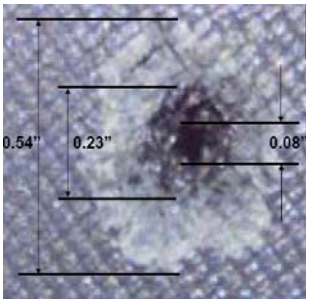


HST Repair Logistics

When the HST service mission was added to the manifest in 2006, the rescue vehicle—which was also manifested along side the HST vehicle—was supposed to include a full complement of Thermal Protection System (TPS) repair kits. The repair kits included a full set of Reinforced Carbon-Carbon (RCC) plugs, an overlay kit, a Non-Oxide Adhesive Experimental (NOAX) repair kit, a Tile Repair Ablator Dispenser (T-RAD) kit, and an Emittance Primer Coating (EPC) repair kit. A full complement of TPS repair kits would require the RCC plugs and overlay kit to either be manifested down from the ISS and returned following the HST mission or require another set to be manufactured. Both options have significant cost associated with them; therefore, the plan became to manifest a standard set of repair kits on the rescue mission, which would not include the RCC plugs or the overlay kit. If the rescue mission needed either of those repair kit items, they would have to be transferred from the HST vehicle. The new plan increases the risk to the rescue vehicle if the exact same repair that is done for the HST vehicle is needed for the rescue vehicle. In May of 2008, the HST Mission Director asked the Analysis Group to provide the probability that the rescue mission would need either an RCC plug or an overlay kit given that either one had been used on the HST vehicle and failed—therefore requiring a rescue mission in the first place. The Analysis Group was able to fulfill this request and showed the probability was small; therefore, requiring the rescue vehicle to carry a full complement of TPS repair kits is unnecessary.

HST Micrometeoroid and Orbital Debris (MMOD) Assessment

The MMOD risk for the HST mission is significantly higher than the MMOD risk associated with an ISS mission due to the altitude of the HST vehicle and the attitude the Orbiter must fly to perform the HST repairs. Therefore, NASA has put forth a considerable amount of thought and effort into mitigating the HST mission MMOD risk. One of the more effective mitigations is to perform an Orbit Adjust, which would place the Orbiter in a lower altitude and lower the debris flux after the HST repair mission is complete.



NASA's Astromaterials Research and Exploration Science Group assessed the HST MMOD risk with and without assuming an Orbit Adjust, and the Analysis Group presented the delta risk to the Orbit Flight Techniques Panel (OFTP) as compared to the Shuttle PRA top risks. The Analysis Group emphasized that although the delta risk may appear small when compared to the overall MMOD risk, it is a significant risk when viewed by itself. Based on the Analysis Group's presentation of the delta risks, the

OFTP changed their opinion from being in favor of not performing the Orbit Adjust to in favor of performing the Orbit Adjust since there is only a small risk increase associated with reduced emergency landing sight coverage. The current plan is to nominally perform the Orbit Adjust for the HST mission.

Crew Rescue Analysis for STS-122, 123, 124, and 126

After the loss of Columbia (STS-107), NASA requires Flight Day 2 (FD 2) inspections to survey TPS damage on the Orbiter. Depending on the severity of the TPS damage, the Mission Management Team (MMT) decides whether to repair the damage on orbit or declare CSCS on the ISS, which requires a rescue mission by a standby Shuttle. Prior to STS-118, the MMT asked the Analysis Group to evaluate the likelihood of a successful crew rescue attempt if the crew had to perform CSCS on the ISS. The MMT requested this study to help them make risk-informed decisions about whether to declare CSCS in emergency deorbit scenarios after the FD 2 inspections. In addition, the MMT could have also used this study to weigh the risks if they were faced with the decision to repair the TPS damage or declare CSCS for STS-118.

The STS-118 crew rescue analysis showed that crew rescue success is dominated by the potential for a launch delay that is greater than the stay on the ISS since the ISS has limited consumables such as oxygen. The STS-118 analysis also showed that crew rescue is heavily dependent on the rescue vehicle's status in processing at the time of launch. As a result of the effort and findings from the STS-118 analysis, the MMT asked the Analysis Group to continue providing this assessment for each subsequent mission as a risk metric.

In 2008, the Analysis Group provided crew rescue estimates for four missions, STS-122, STS-123, STS-124 and STS-126. The most notable was the analysis performed for STS-124, because there was a gap between the CSCS duration on the ISS and the Launch on Need (LON) vehicle processing time. To close the gap and show a positive CSCS margin for reducing the risk, credit was given for progress resupply and the new Oxygen Generation System (OGS) on the ISS. The STS-124 crew rescue analysis also showed how the crew rescue risk can be improved by sending the crew home on the Soyuz. In addition to the standard crew rescue analysis for STS-126, the Analysis Group also provided a histogram of the crew rescue risk analyses since STS-118 to aid in comparing the current mission risk to past missions.

MMOD Late Inspection Benefit Analysis

In 2003, NASA began on-orbit inspections of the Orbiter to reduce the risk from ascent debris and/or MMOD damage. Late inspection is at risk periodically because it is manifested near the end of the mission and previous mission events may require more time than expected; thus, late inspection is a candidate for removal due to mission schedule reasons as the crew's life support systems approach their limits. Late inspection is on the Analysis Group's list of assessments for each mission to keep Shuttle management aware of the potential risks when decisions to change and/or remove late inspection arise.

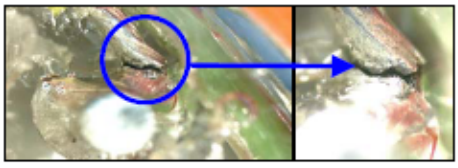
Safety Problem Investigation Team Support

The Safety Problem Investigation Team (SPIT) was created after the Columbia accident to serve as a realtime responder to Shuttle and related ISS anomalies that occur from the beginning of the launch countdown to completion of post landing procedures. The SPIT supports a formal process for providing results, conclusions, and recommendations to the S&MA MMT representative. The SPIT also provides summary information to the Safety Mission Evaluation Room (MER) console for disclosure to the MER manager and other MER console positions.

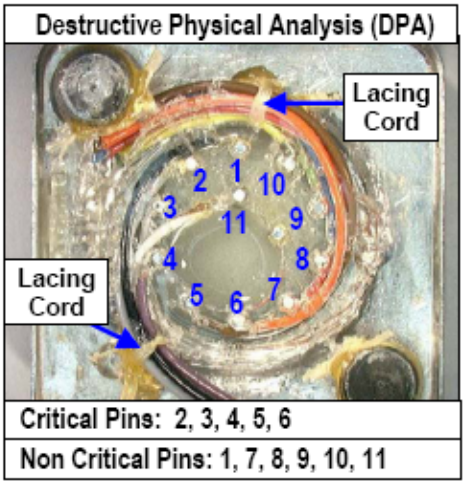
The Analysis Group provides support to the SPIT by creating fault trees to help diagnose the root causes of an anomaly (i.e., "Cause Trees"), or by providing requested probabilities from the Shuttle PRA. During STS-124, the Analysis Group developed a "Cause Tree" for the "Left Orbital Maneuvering System (OMS) Secondary Thrust Vector Control (TVC) Reads Zero" anomaly. During STS-123, the fuel tank pressure on Auxiliary Power Unit (APU) 1 was decaying. The flight rules directed the APU should run to depletion in case the pressure decay was the result of a hydrazine leak. However, if the APU was allowed to run to depletion; only two APUs would be available for entry, which also posed a risk. Therefore, the SPIT requested the Analysis Group to provide various probabilities to assist in deciding whether to run APU 1 to depletion. These SPIT analysis activities are just two examples of SPIT support the Analysis Group provided in 2008. The Analysis Group will continue to provide this much needed support to the SPIT for each flight.

Solid Rocket Booster (SRB) Power Bus Isolation Supply Analysis

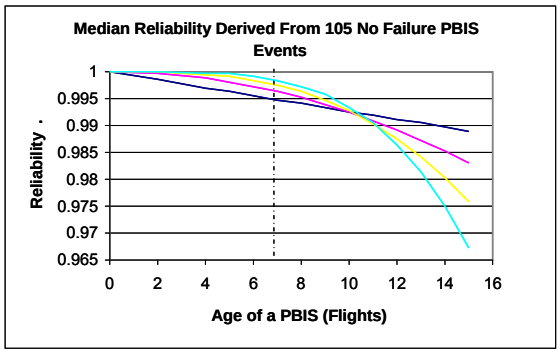
During the STS-124 Flight Readiness Review, the SRB Project Office brought forward the status of an ongoing analysis that was being conducted for a broken wire in a T2 transformer within the SRB Power Bus Isolation Supply (PBIS) module. The PBIS module provides SRB bus power to Criticality 3 instrumentation. Although the broken wire was associated with a non-critical pin within the T2 transformer, the failure mode was applicable to a critical pin. If a similar failure occurred during flight to a critical pin, the resulting open circuit would lead to a short that would cause an SRB Bus loss (worst case) or a Hydraulic Power Unit (HPU) loss (more likely case). Common cause failure would result in losing two HPUs, which would lead to Loss of Crew and Vehicle (LOCV). When inspecting the 12 T2 transformers, 43% of the applicable T2 transformer pins showed indications of cracks. The Analysis Group used the crack and short data, along with demonstrated flight history, to assess the risk on STS-124, STS-125, and



Wire Broken at Pin 10 Post



PBIS T2 Transformer Leads



STS-126. The Analysis Group's assessment results were compared to the SRB Project Office assessment as well as an MSFC S&MA assessment. The major difference between the Analysis Group assessment and the SRB Project Office assessment is that the Analysis Group assumed the failure rate is increasing overtime (i.e., older PBIS modules have a higher probability of failure than younger PBIS modules). This comparison highlighted the amount of uncertainty associated with assessing the Shuttle risk associated with PBIS failure. Although the SSP accepted the risk associated with a broken wire in the SRB T2 transformer for the next four flights, the Analysis Group's assessment emphasized the need to implement a design change that would eliminate the failure in future flights.

Shuttle PRA Update, Iteration 3.0

The Analysis Group completed a major update to the Shuttle PRA in 2008. This update included a complete overhaul of the functional data to have traceability of the pre-priors. Pre-priors are data sources that are used to develop a prior that is then either used in the Shuttle PRA or is Bayesian updated with Shuttle-specific data. The Iteration 3.0 update also expanded the Shuttle PRA model scope to include aborts and rendezvous and docking. Preliminary Shuttle PRA results were presented to the PRCB in May 2008 as part of the Shuttle Top Risk Review. After receiving feedback during the PRCB presentation, updates were made to Iteration 3.0 and the results were finalized in November 2008. The Analysis Group initiated review summits in December 2008 with the Orbiter Project Office, Mission Operations Directorate, and Safety and Mission Assurance; which are scheduled to be complete in January 2009. Feedback from the review summits will be incorporated into an Iteration 3.1 update that is due out in 2009.

Flight Software PRA

The Analysis Group developed a methodology for assessing Shuttle Flight Software (FSW) risk. The Shuttle FSW PRA takes into account over 30 years of SSP quality management data from United Space Alliance (USA), including ground (simulation), flight testing, and verification data. The FSW PRA also takes into account different production and execution rates of new and latent errors as well as the maturing of the FSW test and verification process. Using the FSW PRA estimates, the Analysis Group was able to establish a range of LOC probabilities from Orbital Increment (OI)1 through OI30 (current). The Analysis Group's FSW PRA was compared to USA's LOC risk assessment, and the two were deemed not to be statistically different. The results and methodologies in the Analysis Group's FSW PRA were well accepted within the Shuttle and Constellation Programs. The FSW PRA results will be used in the next iteration of the Shuttle PRA. Constellation is using the Shuttle FSW PRA as a benchmark to assist in determining the best methodology for analyzing Constellation software risk.

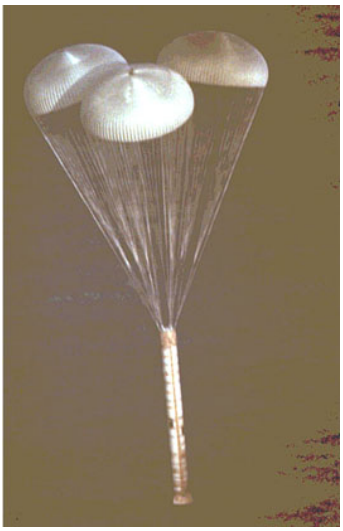
Precursor Analysis

The Office of Safety & Mission Assurance (OSMA) at NASA Headquarters requested the Analysis Group and other SSP S&MA entities combine efforts to perform a precursor analysis pilot project. A precursor is an indication of a problem that could recur with more severe consequences. An example of a precursor is a hydrazine leak, indicative of a loose fitting, which if not corrected, could lead to a larger leak and fire.

Information Systems Lab (ISL), a contractor for NASA Headquarters' OSMA, developed an initial precursor analysis process that was based on U.S. Nuclear Regulatory Commission (NRC) established procedures. The ISL initial precursor analysis process was tested and refined by evaluating Shuttle Orbital Maneuvering System/Reaction Control System (OMS/RCS) Corrective Action Reports in a collaborative workshop held at JSC November 13-16, 2007. A follow-on workshop to this precursor screening/disposition exercise was held March 3-7, 2008. This precursor screening/disposition exercise focused on In-Flight Anomalies (IFAs) generated from STS-114 through STS-116 and included input from JSC System Engineers, the Analysis Group, other personnel from JSC S&MA, and ISL. IFAs were dispositioned as no action, trend, or further analysis. Rule-based screening guidelines created during the first workshop were further developed to facilitate the quick disposition of anomalies. JSC support made this exercise a success by generating significant technical discussions and identifying process improvements.

Shuttle R&M Tasks

SRB Parachute Material Reliability Analysis



The SRB parachutes provide the means for decelerating the SRB and allowing it to impact the water at an acceptable speed. Each SRB has one pilot, one drogue, and three main parachutes. The Analysis Group conducted an assessment to examine the reliability of the SRB large main and drogue parachute material.

Using the failure history for both types of parachutes, logistic regression analysis confirmed the SRB large main parachutes have shown reliability growth since their introduction and have achieved a high level of reliability. The analysis also confirmed the drogue chutes are at a high level of reliability. The results of this analysis will be used to support the recovery system design for the CxP.

Orbiter Problem Trend and Risk Analysis Report

The Analysis Group prepares the JSC PRACA data for trending analysis bi-annually to ensure the most current Corrective Action Reports (CARs) are included in the analysis. The Analysis Group sends all new records to the S&MA Subsystem Engineers. The engineers screen the records and add information relevant to trending. After engineering review, the Analysis Group incorporates the new records in the existing database. The Analysis Group then performs two statistical analyses. The first analysis identifies part groups with significantly increasing rates of problem occurrence in the form of a trend score. The second analysis assigns a risk age index of high, medium, or low to each open CAR. Any part group with a significantly increasing trend score or high risk open CAR is reviewed by an S&MA Subsystem Engineer and included in the bi-annual *Orbiter Problem Trend and Risk Analysis Report*. This report is submitted to the Orbiter Project Office to assist them in identifying areas that should be investigated on the Orbiter.

Additionally, the Analysis Group is investigating text data mining tools and techniques to assist in identifying longstanding and recurring problems that present a risk to the remaining flights.

Point Sensor Box Analysis

The Point Sensor Box (PSB) is used in the Orbiter's Main Propulsion System (MPS) to monitor eight liquid hydrogen and liquid oxygen sensors, known as level or point sensors, that are used when filling the External Tank. The PSB determines whether the level (or point) sensors are wet or dry. The PSB also monitors four liquid hydrogen and four liquid oxygen ECO sensors, called depletion sensors, and translates the sensors states into messages to the Orbiter's General Purpose Computers (GPCs). The GPCs use the sensor states to shut down the SSMEs in the event a propellant quantity is depleted prior to nominal Main Engine Cutoff (MECO).

The Analysis Group analyzed the anomaly history of all seven PSB flight units to estimate the accumulated operating time, the failure rate trend, and the conditional reliability of the PSBs during the launch pad and flight time periods. This analysis also assessed the aging factors of the electronic components in the PSBs.

Failure data indicates the PSBs may be in an early wear out phase and their reliability may deteriorate as additional operation time accumulates. However, an examination of the PSB key electronic components shows no appreciable aging in the components. All components are high-quality, established reliability parts that have been vigorously qualified and tested. The PSB analysis results were used to gain a better understanding about the recurrent Shuttle ECO sensor problem and to determine if the PSBs could be eliminated as a contributing source to the ECO sensor failures.

Shuttle Data Management Tasks

The Analysis Group developed two new databases, one geared toward PRA activities and the other geared toward R&M activities. The PRA database is a searchable Access® relational database that brings together the major elements of the current Shuttle PRA functional data set (e.g., generic priors, Bayes-Beta, Bayes-Gamma, and failure report classes). The new PRA database also has the capacity to accommodate additional failure rates, CARs, and operational information. In addition to the Access database, the Analysis Group created a new set of comprehensive Excel® files that provide detailed information on the pedigree of the Shuttle PRA likelihood data. The pedigree information includes operation time (or demands), the rational for relevant failures, related discounting, etc.

The new R&M database is an Excel database that consolidates the JSC S&MA R&M input/output data into a menu-driven database that uses a modified vertical-based taxonomy from the Logistics Asset Tracking System.

The new JSC S&MA PRA and R&M databases provide an improved level of traceability, maintainability, and configurability. These databases were presented to the SSP Risk and Reliability Managers and were well received within the JSC S&MA Office; therefore, they will be used to sustain the analysis needs for upcoming manned/unmanned NASA programs and projects.

Constellation

NASA's CxP is building the next generation of spacecraft for human exploration. The Orion crew exploration vehicle will launch on the Ares I launch vehicle. The Ares V will launch cargo for lunar missions. The CxP was established to return humans to the moon by 2020 to set up a lunar outpost in preparation for journeys to Mars and other destinations in the solar system. Orion will be capable of carrying crew and cargo to the ISS. It will also be able to rendezvous with the Lunar Lander and Earth Departure Stage to carry crews to the moon. Eventually, Orion will be used to transfer crews to Mars-bound vehicles.

Since the CxP and its projects are in the beginning stages; the majority of Constellation tasks/efforts are in the early stages of design, testing, construction, and some are even in their early definition phases. The Analysis Group has been involved in many of these tasks/efforts to ensure S&MA products/processes are correctly implemented within the CxP and its projects. The following task summaries recap some of the more significant Constellation PRA and R&M tasks the Analysis Group performed during 2008.

Constellation PRA Tasks

Developing Risk Assessment Methods

Since spaceflight is so unique, many of the identified risks require unique solutions to understand them and estimate their risk. In the SSP, unique models for ascent debris risk, MMOD risk, and other special cases were developed and incorporated into the traditional PRA model. For Constellation, new methods are also being developed to ensure the risks in the new program are understood and minimized. Two new methods are being developed to estimate software risk and to apply common cause in the Constellation risk models.

The *Constellation Program Probabilistic Risk Assessment (PRA) Methodology Document*, CxP 70017 specifies that software will be incorporated in the PRA models, but does not specify the methodology for conducting a software PRA. Software risk has not typically been addressed in PRA models because there is no accepted method to evaluate it. The history of spaceflight shows that software risk is not negligible and should be accounted for in a comprehensive risk model. For new vehicles, like those being designed for Constellation, software risk will be high initially since it is untested in the field until the first flight.

Latent errors may take some time to detect and correct. Therefore, the Analysis Group has been involved in developing and evaluating Constellation software risk methods. As previously mentioned in the Shuttle task summaries, the Analysis Group developed an empirical software risk model that is based on over 30 years of Shuttle software failure data. Since the software model is an empirical model based on Shuttle data, it is not necessarily translatable to evaluate Constellation software risk. However, the Shuttle empirical software risk model is being used as a benchmark to evaluate different existing general methodologies in Constellation's quest to find the best method for analyzing software risk.

Current modeling shows common cause (generic failures) to be a risk driver for some of the Constellation systems. The Analysis Group is leading the effort to ensure consistent modeling across all Constellation projects. In addition, current common cause methods being used rely on generic data from non-aerospace industries. New methods are being developed to tailor the modeling to the specific components and environments seen in Constellation to ensure the most accurate risk rankings and risk estimations possible.

These are just two of several areas in which new methods are being developed for Constellation risk assessments. Other developing methods include abort simulation and reliability growth for launch vehicles. The Analysis Group will continue to participate in the development of new methods as needed to ensure the best analyses are being performed and the most accurate risk estimates are used for design decisions.

Constellation Loss of Crew/Loss of Mission Requirements

The Analysis Group is leading an ongoing assessment to determine the achievability of the Loss of Crew (LOC) and Loss of Mission (LOM) requirements in the *Constellation Architecture Requirements Document (CARD)*, CxP 70000. The assessment began by developing a timeline of hazards for both the ISS mission and the Lunar Sortie mission. The hazard timeline was constructed in the form of workshops with expert participation from project offices, SR&QA, Mission Operations Directorate (MOD), etc. Five workshops have been conducted to date:

- Ares I cryo loading through orbit insertion
- ISS mission from orbit insertion through landing
- Lunar Sortie mission from Low Earth Orbit docking through landing
- Ares I and Orion ground operations from vendor/government hardware turnover to cryo loading
- Contingency EVA

The products of these workshops are timelines (as shown on the next page) of critical functions and the hazards associated with the functions. The Integrated Hazard Analysis Team used these timelines and associated hazards to develop event tree models for the integrated LOC/LOM models. These hazard timelines will also be beneficial in determining if any gaps exist in the project LOC/LOM models and to ensure all integrated LOC/LOM analyses are performed.

EVA Preparations

Functional Event	Don PLSS		PLSS checkout	
Functional Failure (Hazard Topic)	Suit integrity failure (connector failure, seal failure, etc.)	PLSS failure	Suit temperature control/ventilation failure	O2 supply or CO2 removal failure
Hazard	Failure to maintain habitable suit environment results in inability to perform EVA, hazardous crew conditions, and/or abort.			
Hazard Report Developer	EVA	SE&I	EVA	EVA
Stakeholders	EVA, Altair	EVA, Altair	EVA, Altair	EVA, Altair
Comments\ Homework	Assume suits are donned on surface for ascent.		Four hours is the designed requirement.	

The current LOC/LOM integrated analysis incorporates project-developed models from Orion, Ares, and Lunar Lander. Detailed event tree models were developed based on the current mission operational concepts. The models incorporate conditional probabilities for aborts related to the conditional probabilities that a failure is catastrophic from a blast, debris, or thermal considerations for each Ares I failure, as well as the Orion flight performance considerations based on the initial conditions of the Ares I failure. The Orion models are based on the August 25, 2008, Orion model drop. The Ares I model is based on the Ares I Preliminary Design Review (PDR) design. The Lunar Lander fault tree models are developed based on the Lunar Lander Design Analysis Cycle 2 vehicle.

The integrated LOC/LOM analyses results provide an integrated risk ranking of the project models. In addition, a list of gaps can be developed where risks are present but not yet accounted for in the project models. The integrated LOC/LOM analyses also allow the CxP and its projects to determine if the CxP's requirements are being achieved or are impractical to achieve. The Analysis Group will continue to conduct these integrated LOC/LOM analyses as the Constellation projects, associated vehicles, and missions evolve.

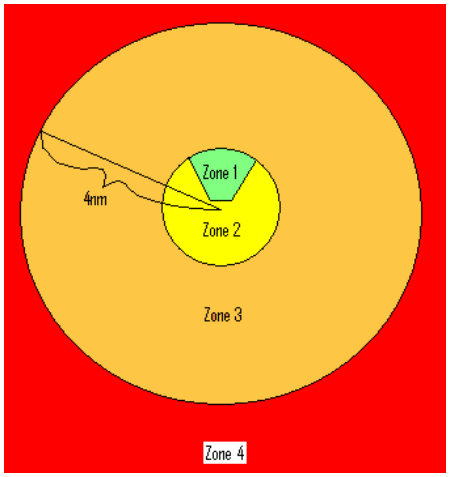
ARES I-X Range Safety PRA

The Probabilistic Risk Assessment Working Group (PRAWG) was chartered in early 2007 as the forum through which all launch vehicle range safety-related reliability analyses and products would be coordinated for the CxP. This technical forum supports the Launch Constellation Range Safety Panel (LCRSP) in all matters related to estimating vehicle failure probabilities for range safety risk assessments in compliance with the requirements of the CxP, NASA's Range Safety Program (as defined in NASA Procedural Requirement 8715.5), and applicable Air Force Range Safety policies and requirements. Members of the Analysis Group participate in the PRAWG, along with representatives from the Launch Vehicle Project Office (Ares, Ares I-X), Mission Operations, S&MA, and the 45th Space Wing.

The PRAWG completed a number of tasks in 2008 to support the Ares I-X fight test vehicle. In particular, the group coordinated all tasks pertaining to the final Ares I-X range safety PRA, which was provided to the United States Air Force to be part of the Ares I-X final flight data package. The Ares I-X PRA was developed by S&MA personnel at JSC (which includes the JSC S&MA Analysis Group), MSFC, and Langley Research Center (LaRC).

The Ares I-X range safety PRA was a new challenge because Ares I-X is the first of a kind vehicle. Historically, a vehicle's first flight is usually significantly riskier than mature vehicles due the unknowns associated with first flight. The PRAWG is developing a new process to estimate a first flight failure probability based on PRA models that are normally developed to estimate mature system risk. The methodology being developed links the mature vehicle risk estimate from the PRA model to the empirically derived first flight risk of 0.3 for experienced rocket developers, and adjusts the PRA result based on the difference in complexity of the new vehicle to the generic vehicle risk of 0.3. The work and collaboration between NASA and the 45th Space Wing on this issue will continue to evolve.

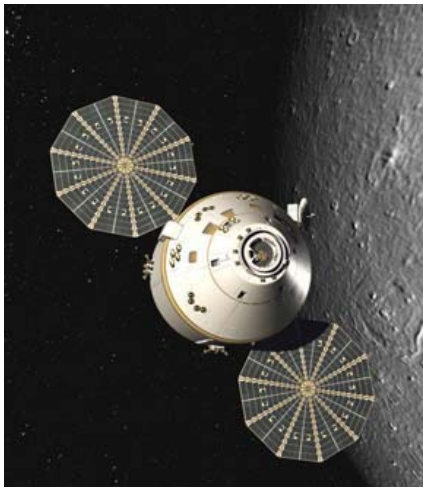
Orion Launch Abort System PRA



As part of the Orion Launch Abort System development effort, several flight tests are planned to prove concepts and operational capabilities. Pad Abort 1 (PA-1) is the first flight test and is scheduled for 2009 at the White Sands Missile Range (WSMR). As part of this test, the risk to personnel, high value facilities, and the general public must be addressed to ensure the risks are within Army requirements. Using standard accepted PRA methods, the Analysis Group estimated the risk associated with the PA-1 flight test as it relates to range safety at WSMR. In particular, the Analysis Group's PA-1 PRA estimated the risk associated with three separate zones defined to categorize potential off-nominal debris that could occur during the PA-1 flight test. The PA-1 PRA provides estimates for each off-nominal debris zone with and without first flight adjustment factors. First flight adjustment factors were included to account for the lower reliabilities associated with a new vehicle's first launch.

The PA-1 PRA results were submitted to WSMR to incorporate in their casualty expectation analysis. Based on the outcome of their analysis results, WSMR will decide whether to proceed with the PA-1 flight test.

Orion Lunar Sortie PRA Review



As the developing contractor, Lockheed Martin is required to submit an Orion Lunar Sortie PRA as a PDR deliverable. The Analysis Group is responsible for reviewing this PRA. The Orion Lunar Sortie is a complex PRA since it includes the integration of many sophisticated and unique systems as well as covers several mission phases. Therefore, Lockheed Martin has committed to making several status drops of the PRA to help ease communication and understanding between Lockheed Martin and the Analysis Group as the PRA is being developed. The status drops and open communication should reduce the amount of Review Item Discrepancies (RIDs) and comments during the Orion PDR.

The first Orion Lunar Sortie PRA drop occurred on July 21, 2008. The main objective in this PRA review was to demonstrate to Lockheed Martin the Analysis Group's expectations for the PDR by treating this status review as if it were in a formal review process. In this status review, the Analysis Group was able to familiarize Lockheed Martin

with the criteria by which they would be judging the Orion Lunar Sortie PRA as well as all subsequent PRAs during the PDR. An additional benefit to this status review was the Analysis Group used this exercise as a means to provide additional training to its PRA analysts in the formal PRA review process. Review comments were submitted to Lockheed Martin. The Analysis Group emphasized how the review comments should not be viewed as shortcomings (especially since the PRA was in its beginning stages), but should be the focus of concentration when continuing to develop the Orion Lunar Sortie PRA for PDR. Another status drop is scheduled for February 13, 2009. During that review, the Analysis Group will verify their comments are being addressed and continue to communicate with Lockheed Martin on the development of the Orion Lunar Sortie PRA.

Orion Post-Landing Emergency Egress Study

The Ground and Mission Operations (GMO) Systems Integration Group (SIG) conducted a trade study to evaluate the post-landing emergency egress design on the Orion spacecraft. As part of their study, the GMO SIG asked the Analysis Group to identify events that would require the crew to exit the spacecraft prior to the arrival of the rescue crew. In addition, the GMO SIG asked the Analysis Group to quantify the probability of occurrence for the events they identified.

The Analysis Group generated a list of credible scenarios that would require an emergency egress, such as water entering the vehicle through various ports and vents; off-nominal conditions inside the vehicle such as smoke, fire, explosion, noxious substance contamination, and carbon dioxide build-up; failure to release the parachutes post-landing; vehicle righting bag failure; etc. The Analysis Group then created a PRA model to quantify the probability of occurrence for each event in the credible scenario list. They used NASA heritage data to develop component failure probabilities, and they worked with meteorologists and the MSFC to assess the probabilities for the phenomenological events (e.g., sea states and sea conditions that would cause the vehicle to roll into an upside down position).

The Analysis Group performed the emergency egress assessment to help the GMO SIG understand the events that would lead to an emergency egress and their likelihood of occurrence, but the Analysis Group also identified mitigations that might reduce those probabilities. The GMO SIG incorporated the results of this assessment into their trade study. One of the most critical findings was that one of the valve openings in the vehicle would lead to nearly unabated flooding in the Orion spacecraft if the vehicle rolled to an upside down position. Based on experience with the Apollo missions, it was determined this event was very likely to occur. The Analysis Group presented this finding to the Constellation Analysis Working Group and Lockheed Martin Engineering, and a redesign of the valve is now being evaluated as part of the next Orion Design Analysis Cycle study.

Lunar Lander Design Analysis Cycle PRAs

The early design of the Lunar Lander (Altair) vehicle is separated into a series of design iterations called design analysis cycles. Lunar Lander Design Analysis Cycle (LDAC) 1 was devoted to designing a minimally functional vehicle; which provided systems that contained no provisions for mission reliability or safety such as redundancy. The common understanding was the LDAC 1 vehicle would never be used and that system safety and reliability would be added in subsequent design iterations.

The LDAC 2 vehicle design targeted the LOC probability or crew safety. The goal of LDAC 2 was to decrease the LOC probability by increasing the reliability of each Altair system. The approach chosen was to perform a series of design architecture trade studies that involved each Altair system and subsystem and also include a consideration of system reliability as the figure of merit.

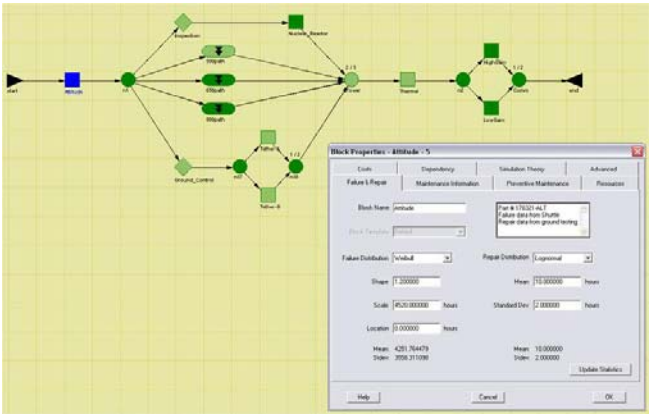
These rapidly progressing trade studies required quick turnaround reliability analysis results to support decision-making in a dynamic project environment. Therefore, the Analysis Group chose a streamlined, spreadsheet-based version of PRA to inform each of the concurrent design studies. Rapid response products included near realtime identification of risk drivers and a quick look at LOC probability versus Altair mass comparative (between each proposed architecture) estimates. The results from these trade studies were used to inform the decisions that led to the closure of the LDAC 2 Altair design. The LDAC 2 final analysis results indicate a LOC probability improvement of two orders of magnitude. This rapid turnaround risk-informed design analysis process attracted favorable attention throughout the CxP and NASA. The analysis process and results were briefed to numerous groups within NASA, including the OSMA Associate Administrator and the NASA Chief Engineer.

The LDAC 3 vehicle design targeted mission reliability, as measured in terms of the LOM probability. The goal of LDAC 3 was to decrease the LOM probability to a level more in line with the Constellation requirement. Once again, a series of design trade studies was deployed and the Analysis Group employed the rapid turnaround spreadsheet reliability estimator. As with LDAC 2, the spreadsheet reliability estimator identified risk drivers and provided insight into the relative risk reductions associated with various system configurations. Final results for LDAC 3 are still in work, but preliminary estimates indicate an improvement of one order of magnitude. The preliminary results also indicate the Constellation LOM probability requirement may not be practical. The Analysis Group will continue to work with Constellation to resolve these Altair LDAC 3 issues.

Constellation R&M Tasks

Constellation Reliability Availability Maintainability Panel Support

The Constellation Reliability Availability Maintainability (RAM) Panel oversees the implementation and verification of all CxP RAM requirements as well as provides expertise for RAM technical assessments and issues. The Constellation RAM Panel also coordinates with the Constellation Safety and Engineering Review Panel (CSERP); CxP PRA Panel; Program Integration, Design, Test, and Systems Engineering; as well as the CxP and its project offices to recommend approvals for RAM products and processes; collaborate for community best of practices; and participate in other collaborative Constellation activities. The Constellation RAM Panel includes members of the Analysis Group, but the Analysis Group also provides modeling and analysis services for the Constellation RAM Panel.



The Analysis Group's support to the Constellation RAM Panel in 2008 included developing a simulation tool to evaluate the relationship between availability for operation versus downtime due to failure and repair. Currently, a data set is being developed for input in a Raptor™ software model to simulate the failure and repair of components within the Constellation elements during a mission. The input data set includes Orion subsystem reliability block diagrams and the functions involved in a mission. The primary output from the Raptor model is "availability" of various subsystems/functions over the entire mission. The purpose of the analysis is to determine unavailability drivers and focus on potential areas to increase availability.

An additional service the Analysis Group provided for the Constellation RAM Panel in 2008 is the development of an Excel-based database that aggregates reliability data from all the Constellation projects to be used for integration purposes at the program level. The goal is to standardize the name of items that have been judged relevant to both the program and project RAM and PRA analyses. The database has the ability to retrieve the data pedigree (e.g., failure rate/mean time to failure) through self-contained hyperlinks. The database is flexible and can grow to support the needs of the Constellation RAM activities.

The analysis Group will continue to participate in and provide expert analytical services to the Constellation RAM Panel in 2009.

Constellation Panel and Working Group Support

The Analysis Group participates in and supports several other Constellation panels and working groups both at the program and project level. The types of activities performed for these panels and working groups is to perform technical assessments as requested, facilitate issue resolution based on assessment findings, provide expert opinions, and review documents. The following are example activities performed for the Constellation panels and working groups in 2008:

- Conducted research and made comparisons between ammonia and Freon for incorporation into a trade study that determined whether the weight reduction provided by using ammonia instead of Freon is offset by the dangers of having ammonia on the vehicle. This research and comparison assisted in identifying the necessary precautions and controls for using ammonia.
- Provided input for the change request to improve existing requirements in the *Constellation Program Integrated Safety, Reliability, and Quality Assurance Requirements Document*, CxP 70059. Many of the Analysis Group's inputs were considered and incorporated into the document, resulting in stronger R&M requirements for the CxP.
- Compared NASA-wide and CxP-specific requirements to the developing contractor's documents/plans to identify any omissions or shortcomings in meeting either the agency's or program's requirements. The developing contractor documents/plans reviewed included: R&M plans and reports, maintainability and supportability outlines, and PDR planning presentation.
- Provided expert opinion to assist SE&I in developing the data for their launch availability model.

Orion Service Module Fairing Analysis

The Service Module (SM) fairings are panels that cover and protect the SM components. These panels are load-bearing panels in the SM structure. The Constellation Group in JSC's Program Engineering Integration Office was tasked to conduct the SM Load Bearing Study, where the objective was to investigate cost-effective methods for maintaining the components under the SM fairings during ground processing. In their efforts to conduct the cost-benefit portion of this study, the Constellation Group asked the Analysis Group to estimate the likelihood that the components housed under the SM fairings would require maintenance. The Analysis Group derived the probability of a maintenance event using exposure times and component failure rates. Failure rates were determined for over 1,200 SM components using NASA heritage data and commercial data sources. The failure rates estimated with commercial data sources were normalized to account for the space environment and associated manufacturing quality. Once the component failure probabilities (or maintenance event probabilities) were determined, the Analysis Group ranked the top contributors. The Analysis Group submitted their results to the Constellation Group and the Orion SR&QA Panel to assist in the decision-making process for modifying the current SM fairing design.

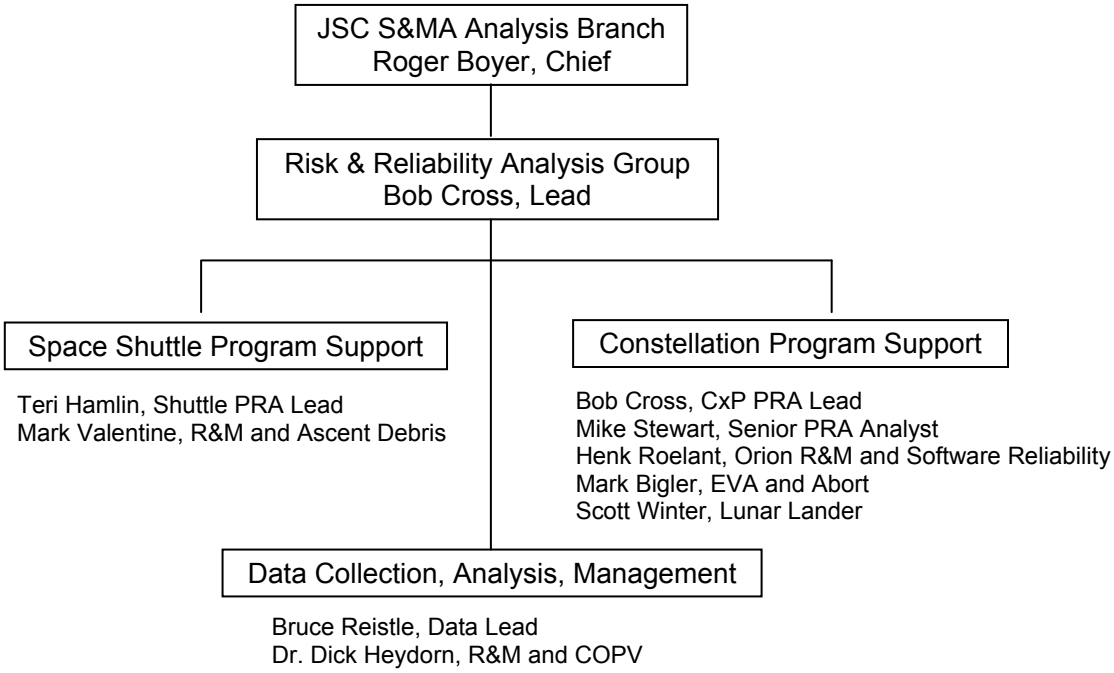
ANALYSIS GROUP STAFF

The Analysis Group always strives to produce the highest quality services and products in a timely and cost-effective manner. The experience base within the Analysis Group staff provides the group with the utmost risk and reliability experience in performing assessments and analyzing data for the majority of NASA's current and future space exploration activities.

The Analysis Group is comprised of the JSC S&MA Analysis Branch staff and S&MA support services contractors. The JSC S&MA Analysis Branch staff serves as the lead for the various Shuttle and Constellation analysis tasks performed within the Shuttle and Exploration Division, and the support services contractors perform numerous analytical activities on behalf of the JSC S&MA Analysis Branch.

JSC S&MA Analysis Branch

The chart below displays the organizational structure for the JSC S&MA Analysis Branch. A professional biography summarizing each JSC S&MA Analysis Branch member's qualifications and accomplishments is also provided.



Roger Boyer — Analysis Branch Chief

Roger has a Bachelor of Science (B.S.) in both Nuclear Engineering and Mechanical Engineering from the University of Missouri—Rolla. He holds a Master of Science (M.S.) in Nuclear Engineering also from the University of Missouri—Rolla. He worked for the Union Electric Company at the Callaway Nuclear Plant for three summers in nuclear construction, plant engineering, and nuclear safety analysis, respectively. He then joined Houston Lighting and Power (HL&P) Company on the South Texas Project (STP) in 1983, performing accident analyses in the Nuclear Safety Analysis group and developing the STP PRA. As a PRA analyst, he performed system analyses of several plant systems, developed ESDs and event trees for several initiating events, assisted with the human actions analysis and external events analysis efforts, was responsible for the overall quantification of the plant model, and performed a comprehensive risk-based technical specification assessment for submittal to the NRC. From 1990 to 1994, he developed a high-fidelity thermal-hydraulic simulation of the Space Station Freedom Active Thermal Control System (ATCS) for the McDonnell Douglas Space Systems Company and served as the task manager for the ATCS advanced automation fault detection, isolation, and recovery system project. From 1994 to 1997, he returned to HL&P, where he led the in-house development of its thermal-hydraulic-related nuclear fuel reload safety analyses, performed several computer code verifications, and co-authored a Westinghouse topical report to the NRC.

In 1997, Roger joined the JSC SR&QA prime contractor (SAIC) as a Senior PRA Analyst and soon became manager of its Shuttle Analysis section, directing PRA, trending, and reliability analyses for the SSP. As part of this role, he led a team of 15 groups from 9 different companies and 8 different locations across the country to complete the first SSP-sponsored Shuttle PRA in 2003. He joined NASA in 2003 as the Shuttle Risk and Reliability Group Lead for JSC's SR&QA Directorate. During this tenure, the Shuttle analysis activities more than tripled following the Columbia accident, resulting in a challenge to manage the increased workload while maintaining product quality. In 2006, Roger was promoted to his current position as the JSC S&MA Analysis Branch Chief, combining the new CxP's analysis work with Shuttle's and providing oversight of the safety review panel chairs for both programs. Roger has written/presented several technical papers on thermal-hydraulics, advanced automation, and PRA topics and has served as a technical paper reviewer for several national and international forums. His professional interests include: establishing a high-quality and respected risk and reliability analysis team for NASA; promoting the collection, maintenance, and analysis of data supporting the Analysis Group's assessments; and ensuring the well-being of his teammates.

Bob Cross — Analysis Branch Group Lead and Constellation PRA Lead

Bob has a B.S. and M.S. in Nuclear Engineering from the University of Florida. He joined the Tennessee Valley Authority in 1986, performing thermal-hydraulic and nuclear core design analyses in the Nuclear Fuels group. In 1989, he joined HL&P in a similar position before transferring to the PRA group. In the PRA group, he served as the Principal Investigator for the STP Individual Plant PRA Examination, where he was responsible for system analysis and overall model quantification. At HL&P, Bob also developed the risk model plant operators and maintenance personnel used for realtime risk assessments as well as participated on the plant emergency response team.

In 1996, Bob entered the aerospace industry and began working for SAIC as a Senior PRA Analyst on the JSC SR&QA contract. Later he became a Project Manager at SAIC, developing new business for oil and gas industry risk assessments. As part of this role, he led teams that performed numerous risk assessments related to offshore drilling. In 2001, Bob joined American Bureau of Shipping (ABS) Consulting as a Senior Consultant. During this tenure, he held the lead position responsible for integrating risk-informed decision-making in ABS' shipping industry, which involved developing risk-informed construction guides for ship owners, training ABS personnel, and developing quantitative risk models.

In 2003, Bob returned to the aerospace industry as a Senior PRA Analyst in JSC's SR&QA Directorate. He currently serves as the Group Lead and Constellation PRA Lead in the JSC S&MA Analysis Branch. His current responsibilities include overseeing and directing the analysis activities of the Analysis Group and specifically directing/interfacing with the CxP on all LOC and LOM discussions. Bob has also written/presented several technical papers on risk and reliability topics for several national and international forums.

Mark Bigler — EVA and Abort

Mark Bigler has a B.S. in Electrical Engineering with a minor in Economics from New Mexico State University and an M.S. in Nuclear Engineering from Texas A&M. Mark began his career serving four yeas as an officer in the Nuclear Navy. While in the Navy, he served aboard the USS California as a Mechanical Division Officer and later as an Electrical Division Officer. Mark also served as an Engineering Watch Officer over nuclear propulsion plants in the Navy. After completing his naval tour, Mark joined the reliability engineering group at the STP Nuclear Plant for three years. In this position, Mark was introduced to PRA with his work on the Maintenance Rule, which was a new regulation developed to ensure that maintenance programs at nuclear power plants were more risk-informed. Mark later entered the aerospace industry as a reliability analyst for Lockheed Martin in the system safety group, where he performed Failure Mode and Effects Analysis and hazard analysis on several projects including: the Space Station Airlock Test Article; the Umbilical Interface Assembly for the Quest airlock; A Chamber B human rated test; and the EVA helmet lights, batteries, and associated charger. After leaving Lockheed Martin, Mark worked for SAIC almost 10 years. During that time, he was responsible for several Shuttle system PRAs, including OMS/RCS, ATCS, Environmental Control and Life Support System, and Landing Deceleration. Mark also

worked on an initial EVA PRA proof of concept study to show the benefits of an EVA PRA to both the Shuttle and ISS Programs. Mark also provided valuable input to the Entry Public Risk Assessment using the Shuttle PRA results. In his last two years at SAIC, Mark served as PRA Analyst Technical Lead. In that role, Mark provided guidance to the support services contractor PRA group; oversaw a PRA team that updated the Shuttle PRA; reviewed PRA group analyses; started developing CxP and Orion PRA models for both Lunar Sortie and ISS missions; mentored new employees; developed plans, schedules, and budgets; provided inputs for performance appraisals; and relayed project statuses to management and customers. Mark joined the JSC S&MA Analysis Branch in November 2007. He is currently responsible for risk analyses related to abort, range safety, and EVA. He also provides support to both Constellation Program level and Orion Project level PRA analyses.

Teri Hamlin — Shuttle PRA Lead

Teri has a B.S. in Nuclear/Mechanical Engineering from Worcester Polytechnic Institute. Teri worked at Northeast Utilities for eight years performing PRA activities for their three Millstone Nuclear Power Plants. In 2002, Teri entered the aerospace industry as a PRA analyst for SAIC. At SAIC, she served as the lead for the Shuttle Human Reliability Analysis (HRA), which represents the most comprehensive Shuttle HRA to date. Teri was also responsible for other Shuttle system PRAs at SAIC and also provided backup integration expertise. In 2006, Teri joined the JSC S&MA Analysis Branch as the Shuttle PRA Lead. She is currently responsible for overseeing all Shuttle PRA activities as well as HRA activities for both the Shuttle and Constellation Programs.

Dr. Richard Heydorn — Cx R&M and Composite Overwrapped Pressure Vessel (COPV)

Richard has a Bachelor of Electrical Engineering (B.E.E.) and a Master of Arts (M.A.) in Mathematics from the University of Akron. He also has a Doctorate in Statistics from Ohio State University. After working at Goodyear Aerospace, North American Rockwell, and the Battelle Memorial Institute; he joined the Earth Resources Division at JSC to develop pattern recognition methods for estimating wheat production from Landsat satellite data. Following the Challenger accident, he joined the Reliability Division of the Safety, Reliability, and Quality Control Office working on statistical reliability and general statistical problems. He has migrated through numerous changes in the safety and reliability organizational structure at JSC and has continuously made significant contributions to statistical and reliability issues throughout his NASA career. Richard's most current accomplishments include: estimating the reliability of COPVs for the SSP, developing statistical experiment designs for the COPV reliability model in the CxP, and applying generalized regression methods to estimate pistol grip tool torque prediction intervals for evaluating structure assembly tolerance on the ISS. Richard has also taught statistics as an adjunct at the University of Houston—Clear Lake since 1991 and is an adjunct at Rice University.

Bruce Reistle — Data Lead

Bruce has a B.S. and M.S. in Mathematics from Virginia Tech and a Master of Operations Research from North Carolina State. After teaching secondary math for two years, Bruce worked for Intel as a facility design analyst. Bruce later joined SAIC as a reliability analyst. In Bruce's seven years with SAIC, he predominantly worked as a reliability analyst for Shuttle projects. He served as data analyst and was the primary author of six reliability reports and co-authored several others. In 2007, Bruce joined the JSC S&MA Analysis Branch as the Data Lead. In this role, he is responsible for PRA data including collection, analysis, and structure. Bruce also develops ad-hoc Monte Carlo models such as the Ascent Debris Assessment Model, which assesses the probability of having a critical damage to the Orbiter's lower surface tiles; and the LLCO model, which determines the probability of prematurely depleting the liquid hydrogen supply and hence requiring use of the ECO sensors.

Henk Roelant — Orion R&M and Software Reliability

Henk has a B.S. and a Master of Engineering (M.E.) in Electrical Engineering from Old Dominion University. He began his civil servant career with the Department of Defense as the reliability engineer for the Relocatable Over-the-Horizon Radar Program under the In-Service Engineering Agent. Henk joined NASA in 1990 at LaRC as a reliability engineer. From 1990 to 2001 at LaRC, he served as the Lead Reliability Engineer for the Office of Mission Assurance and was responsible for assessing the mathematical reliability of aeronautical projects/programs and spaceflight products that fell under the auspices of NASA LaRC as well as developing assurance methodologies, processes, and related tools as they relate to reliability. A major highlight in Henk's tenure with LaRC was working on the Galileo/Aerospace System Safety Assessment Program software fault tree analysis tool, which was initially completed in 2001. This tool was developed to provide a large system-level analysis of an entire transport aircraft where subsystem failure independence did not have to be assumed. In 2001, Henk transferred to JSC as a reliability engineer, working on Shuttle PRA and R&M projects. He is currently working with a team of analysts to quantify software risk for the CxP and provides analytical support to the Orion Project Office.

Michael Stewart — Senior PRA Analyst

Mike Stewart has a B.S. in Aerospace Engineering from Iowa State University and an M.S. in Mechanical Engineering from Wichita State University. He received a Master's equivalent degree in Nuclear Engineering from the U.S. Navy in the Nuclear Power School and Prototype Training Program for Officers. He also holds a Professional Engineering License. Mike's professional experience includes: serving as an Officer on a U.S. Navy Nuclear Submarine, working at several commercial nuclear power plants as a manager and individual contributor, working at national laboratories as a project and program manager, working as a project manager at the Institute for Nuclear Power Operations, and providing peer review for multiple PRAs. Throughout his career, Mike has been involved in operations, design, maintenance, and analysis.

Mike has extensive PRA experience and has made significant contributions to current PRA practices and procedures. While employed at the Idaho National Engineering Laboratory, he participated in the early reviews of Wash-1400, which was recognized as the first modern full scope PRA. Mike served as an Analysis Manager at several nuclear power plant utilities that included Computational Fluid Dynamics (CFDs), structural analysis, and PRA. He was involved in the early development of RELAP and RETRAN (two CFD codes). Mike was also instrumental in getting the commercial nuclear industry to adopt a peer review process. He prepared the documentation for a nuclear power plant PRA, which was used as a pilot to prepare the peer review standard that is currently used by the commercial nuclear industry. In addition, both the Electrical Power Research Institute and American Society for Mechanical Engineers have developed PRA standards that were originally adapted from Mike's documentation for the aforementioned nuclear power plant PRA. The power plant for which Mike prepared the PRA documentation still holds the highest score for peer review of any plant. An additional plant that employed Mike also has one of the highest scores for their PRA as a result of documentation changes that Mike oversaw. Mike has also authored several nuclear regulatory guidelines (NUREGs) for the NRC. He was an early contributor to HRA and worked on the nuclear industry-supported Oconee PRA. As a consultant, Mike worked in the petrochemical, transportation, and nuclear industries performing safety analysis and PRA.

Mike transitioned into the aerospace industry 10 years ago as the Lead PRA Engineer for the JSC SR&QA prime contractor, SAIC. In this position, he used his experience and knowledge from documenting PRA as well as establishing peer review to manage the production of the current Shuttle PRA, which is recognized as the best and most complete documented PRA in NASA. Mike later became a civil servant and served as the Lead NASA ISS PRA Analyst. In this position, he re-organized and re-initiated a significant upgrade to the ISS PRA. He was also instrumental in getting the NASA ISS database updated using Bayesian methods, which significantly increased the accuracy of the database predictions. Over the course of his career, Mike has mentored several engineers in the art of PRA and has developed several successful teams that have completed PRAs. Mike is presently conducting reviews for the Orion PRA and has developed a number of the Orion training courses for performing PRA. He reviews the Orion PRA and advises the contractor and NASA management of problems and other items associated with the PRA. He also acts as the interface between Orion Project S&MA and the CxP.

Mark Valentine — Shuttle R&M and Ascent Debris

Mark has a Bachelor of Architectural Engineering (B.A.E.) from Penn State University and an M.S. in Industrial Engineering from the University of Houston. After working in consulting and industry, Mark began working at JSC in 1985. Mark began his NASA career in the Facility Design Division. Since then, he has worked in the Advanced Programs Office, the System Architecture and Integration Office, and most recently within the JSC S&MA Analysis Branch. His current responsibilities include Shuttle and Constellation Program R&M.

Scott Winter — Lunar Lander

Scott has a B.S. in Mechanical Engineering from the University of Missouri – Rolla. Scott joined JSC in 1981 as a Quality Engineer, supporting the SSP. In that position, he worked on a variety of activities from Extravehicular Mobility Unit and Manned Maneuvering Unit design certification to the post-STS 51L Main Propulsion System design assessment.

During his NASA career, Scott also served as Chief of the Shuttle Systems Section in the Quality Assurance Division and later became Chief of the ISS Systems Section in the SR&QA Directorate. While working for ISS, he was assigned as the Chief NASA Negotiator for the Russian Segment R&M requirement.

In recent years, Scott has been performing research into variable specific impulse magnetoplasma rockets—including thermal performance, power balance, and reliability/service life. He now supports the CxP's Lunar Lander Project Office and Lunar Surface Systems Office in overseeing risk/reliability analyses.

JSC S&MA Support Services Contractors

Through the S&MA Support Services Contract (SSC), the JSC S&MA Analysis Branch uses the technical expertise of about 30 engineers and scientists. The team has the education and experience to apply cutting edge mathematics and reliability techniques for S&MA analyses. These techniques include text data mining, Weibull analysis, physics of failure, logistics regression, trend analysis, common cause failure analysis, HRA, and others.

The S&MA SSC brings together engineers and scientists from the leading companies in the safety and reliability industry, including SAIC and SoHaR. SAIC is one of the largest science and technology companies in the U.S. SAIC is the prime contractor and provides management oversight for the JSC S&MA SSC. SAIC also provides most of the PRA contractor staff for the Analysis Group, which are highly trained safety, reliability, and quality PRA analysts and engineers. SoHaR is a leader in the software and hardware reliability industry. SoHaR provides most of the reliability analysts for the Analysis Group. SoHaR also brings RAM-Commander™, a cutting-edge reliability and maintainability prediction tool, to the Analysis Group as well as the expertise in using the software to maximize the tool's capabilities. Together, this contracting team delivers mission-critical products and services to the JSC S&MA Analysis Branch for the Analysis Group's commitment and contribution to safety and success in all of NASA's spaceflight operations.

ACRONYMS

ABS	American Bureau of Shipping
Altair	Lunar Lander
APM	Ascent Performance Margin
APU	Auxiliary Power Unit
ATCS	Active Thermal Control System
B.S.	Bachelor of Science
CAR	Corrective Action Report
CARD	Constellation Architecture Requirements Document
CFDs	Computational Fluid Dynamics
COPV	Composite Overwrapped Pressure Vessel
CSCS	Contingency Shuttle Crew Support
CSERP	Constellation Safety and Engineering Review Panel
CxP	Constellation Program
ECO	Engine Cutoff
EPC	Emittance Primer Coating
ESD	Event Sequence Diagram
EVA	Extravehicular Activity
FB	Fuel Bias
FD 2	Flight Day 2
FRP	Flight Performance Reserve
FSW	Flight Software
GMO	Ground and Mission Operations
GPC	General Purpose Computer
HL&P	Houston Lighting & Power
HPU	Hydraulic Power Unit
HRA	Human Reliability Analysis
HST	Hubble Space Telescope
IFA	In-Flight Anomaly
ISL	Information Systems Lab
ISS	International Space Station
JSC	Johnson Space Center
KSC	Kennedy Space Center
LaRC	Langley Research Center
LCRSP	Launch Constellation Range Safety Panel
LDAC	Lunar Lander Design Analysis Cycle
LLCO	Low Level Cutoff
LOC	Loss of Crew
LOCV	Loss of Crew and Vehicle
LOM	Loss of Mission
LON	Launch on Need
MECO	Main Engine Cutoff
MER	Mission Evaluation Room
MMOD	Micrometeoroid and Orbital Debris
MMT	Mission Management Team

MOD	Mission Operations Directorate
MPS	Main Propulsion System
M.S.	Master of Science
MSFC	Marshall Space Flight Center
NASA	National Aeronautics and Space Administration
NECS	NASA Engineering and Safety Center
NOAX	Non-Oxide Adhesive Experimental
NPR	NASA Procedural Requirement
NRC	Nuclear Regulatory Commission
NUREGs	Nuclear Regulation Guidelines
OFTP	Orbit Flight Techniques Panel
OGS	Oxygen Generation System
OI	Orbital Increment
OMS	Orbital Maneuvering System
OMS/RCS	Orbital Maneuvering System/Reaction Control System
OSMA	Office of Safety and Mission Assurance
PA-1	Pad Abort 1
PBIS	Power Bus Isolation Supply
PDR	Preliminary Design Review
PRA	Probabilistic Risk Assessment
PRACA	Problem Reporting and Corrective Action
PRAWG	Probabilistic Risk Assessment Working Group
PRCB	Program Requirements Control Board
PSB	Point Sensor Box
PWR	Pratt and Whitney Rocketdyne
R&M	Reliability and Maintainability
RAM	Reliability Availability Maintainability
RCC	Reinforced Carbon Carbon
RID	Review Item Discrepancy
S&MA	Safety and Mission Assurance
SAIC	Science Applications International Corporation
SE&I	Systems Engineering and Integration
SIG	Systems Integration Group
SM	Service Module
SPIT	Safety Problem Investigation Team
SRB	Solid Rocket Booster
SR&QA	Safety, Reliability, and Quality Assurance
SSC	Support Services Contract
SSME	Space Shuttle Main Engine
SSP	Space Shuttle Program
STP	South Texas Project
STS	Space Transportation System
TPS	Thermal Protection System
T-RAD	Tile Repair Ablator Dispenser
TVC	Thrust Vector Control
USA	United Space Alliance
WSMR	White Sands Missile Range

National Aeronautics and Space Administration

Johnson Space Center
2101 NASA Parkway
Houston, Texas 77058
http://www.nasa.gov/centers/johnson/home/index.html

www.nasa.gov